Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier xx.xxxx/ACCESS.xxxxxx

Cooperative Estimation of Primary Traffic under Imperfect Spectrum Sensing and Byzantine Attacks

AHMED AL-TAHMEESSCHI[1], MIGUEL LÓPEZ-BENÍTEZ[1], VALERIO SELIS[1], DHAVAL PATEL[2], and KENTA UMEBAYASHI[3]

[1]Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, United Kingdom
[2]School of Engineering and Applied Science, Ahmedabad University, Ahmedabad, India
[3]Graduate School of Engineering, Tokyo University of Agriculture and Technology, Tokyo, Japan

Corresponding author: Ahmed Al-Tahmeesschi (e-mail: ahmedaa@liverpool.ac.uk).

ABSTRACT Cognitive Radio (CR) systems exploit the accurate knowledge of primary traffic statistics to improve CR performance and reduce harmful interference on primary network. It is essential for cooperative CRs to operate in an efficient secured manner while estimating the primary statistics. In this context, a new reporting mechanism for cooperative estimation of primary traffic is proposed to increase the spectrum and energy efficiency. This is achieved by the reduction of the reporting channel overhead from cooperative users to the fusion centre. Simulation results show that the proposed scheme reduces significantly the signalling overhead, thus making the system more spectrum and energy efficient. Moreover, the openness of cooperative CR makes it susceptible to data falsification attacks, also known as Byzantine attacks. This attack poses a series of damages on the reliability of the estimation of primary traffic. In this work, we define the types of malicious coordinated attacks on CRs and analyse the possibility of estimating the primary traffic statistics under these attacks. Moreover, we provide a simple yet effective counter-measure based on the proposed reporting for cooperative estimation. Simulation evaluation shows that the proposed algorithm provides an excellent counter-measure for spectrum sensing data falsification attacks.

INDEX TERMS Byzantine attacks, cognitive radio, cooperative primary activity estimation, differential reporting.

I. INTRODUCTION

COGNITIVE Radio (CR) is a promising solution for the spectrum scarcity problem by having secondary users (SUs) to access primary users (PU) channel (spectrum holes) in an opportunistic and non-interfering manner [1]. Spectrum sensing is a key enabling technique for CR operation, as it allows SUs to detect the presence/absence of PU traffic, which is essential to reduce the interference [2], [3]. An essential requirement for SU is to work in a fast and accurate manner while identifying empty slots in the primary channel. One way of improving the performance of SUs is having knowledge of previous spectrum occupancy pattern (e.g., distribution of idle/busy periods) which can be exploited to improve the system performance [4]. Primary traffic statistical information is essential to access the spectrum in a fast and efficient manner by the selection of the most appropriate channel for transmission [5], enhancing the forecasting of PU occupancy patterns to minimize the interference [6], [7], adjust the energy detection threshold [8] or fight against attacks [9].

The PU traffic activity is initially unknown to SUs and is estimated using spectrum sensing decisions. SUs sense the PU channel periodically and in every sensing event a binary decision (idle/busy) is made based (in case of hard decisions) on an appropriate spectrum sensing (signal detection) algorithm [10]. While the main purpose of spectrum sensing is the detection of transmission opportunities [11], the sequence of spectrum sensing decisions can also be used to estimate the durations of idle/busy periods and their statistics [12].

Nevertheless, primary traffic statistics estimation is hindered by several practical limitations that determine the accuracy to which such statistics can be known by the CR system [13]. This includes the use of a finite sensing period, which imposes a fundamental limit on the temporal resolution in

which the idle and busy periods can be measured [14]. Moreover, channel statistics need to be inferred based on a limited number of channel observations (samples) [15] and spectrum sensing is mainly impaired by sensing errors (i.e., false alarms and missed detections) [16]. Cooperative sensing is proposed to improve the operation of spectrum sensing, taking advantage of spatial diversity at every receiving SU. By cooperation, SUs share their local decisions to make a more accurate global decision of the primary channel state [17], [18]. In this work, cooperative sensing is utilised to provide an accurate estimation of the primary traffic (in particular, the distribution of idle/busy periods) under imperfect spectrum sensing (ISS). Notice that the problem of cooperative spectrum sensing, where the target is to improve the overall detection of PU signals, has received an enormous deal of attention in the literature. By contrast, the focus of this work is on cooperative primary traffic estimation, where the target is to accurately estimate the primary traffic statistics (based on spectrum sensing) by means of cooperation among several SUs, which has received significantly less attention.

The improvement in performance achieved by cooperation is hindered by the increase of cooperation overhead. Several studies aimed at improving energy efficiency in cooperative spectrum sensing by the reduction of consumed power at each step of the cooperative sensing operation [19]. For instance, reducing the power consumed during the sensing stage [20], [21], or at the reporting stage [22]–[24] by selecting the most useful SUs for local states reporting to the fusion centre (FC). In this context, we propose a new reporting mechanism with the aim of reducing the number of required transmissions at each reporting stage (from SUs to FC). This is accomplished through differential reporting where the SUs only report when there is a change in the local channel state observed by each SU (i.e., channel state goes from busy to idle or vice-versa).

Another problem that has not attracted enough attention is the estimation of primary traffic statistics under spectrum sensing data falsification (SSDF) attacks [25]. CR systems are more susceptible to SSDF attacks (also known as Byzantine attacks) and to the presence of greedy users who send false reports to gain more access to primary channels. Multiple studies have considered the effect of attacks on the sensing process [26]–[28] with methods to detect the SSDF attacks [29]. While their main aim is the estimation of the probability of primary signal detection, in our work the main aim is to study the effect of these attacks on the estimation of primary traffic statistics, which to the best of the authors' knowledge has not been investigated in the existing literature even though the topic of CR has been around for over a decade. Other differences can be identified among the proposed work and others. For instance, the algorithm in [26] requires soft decision reports, while ours is based on hard decisions. The algorithms in [27], [28] require multi-stage trust algorithm to identify trusted SUs. In this work, we aim to answer the possibility of estimating PU traffic statistics given this scenario. A simple yet effective algorithm

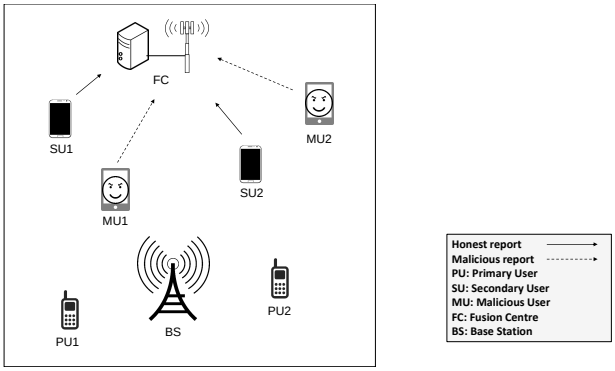


FIGURE 1: System model for cooperative primary traffic estimation with malicious users.

is proposed to eliminate such attacks. In this work, not only we focus on the cooperative estimation of primary traffic under ISS, but also extend the estimation under malicious users (MUs) performing Byzantine attacks. Moreover, we introduce a new algorithm to reduce the amount of overhead in the reporting channel and thereby increase the power efficiency.

The main contributions of this work can be summarised as follows:

1) Study the cooperative estimation of PU traffic statistics under both sensing errors and finite sensing period with experimental validation.
2) Propose a new reporting mechanism (differential reporting) to reduce the overhead in the reporting channel and increase the spectrum and energy efficiency.
3) Study the estimation of primary distribution under both sensing errors and SSDF attacks and propose a new algorithm to counter the effect of such attacks on the estimation of PU traffic statistics. While both aspects have received some attention in the literature separately, they have not been considered simultaneously along with their combined effects on the cooperative estimation of primary traffic statistics.

The remainder of this paper is organised as follows. First, Section II describes the structure of the cooperative system considered in this work along with the estimation of primary signal durations and cooperative algorithms utilised. Different estimation methods for the primary governing distribution are described in Section III. The problem of increasing overhead along with an efficient reporting mechanism are described in Section IV. Section V discusses the problem of SSDF attacks and how to protect against them. The simulation and experimental methodology employed in this work are described in Section VI. The performance of the proposed methods is analysed thoroughly in Section VII. Finally, Section VIII concludes the paper.

II. SYSTEM MODEL AND PROBLEM FORMULATION

In this work, a single PU channel is considered for the sake of simplicity. The PU state holding times (T_0 for idle

periods and T_1 for busy periods) are random variables assumed to be independent and exponentially distributed. The exponential distribution is the most common model used to describe the periods of the on/off states in the literature [30]–[34] even though it has been proven not to be the most accurate since other distributions provide better fit for real scenarios such as the generalized Pareto, Gamma or even more complicated distributions [35]. We use the exponential distribution because it is a special case of the generalized Pareto distribution with a simpler mathematical form. As for cooperative network side, K SUs with a specialised FC are considered along with MUs. The FC is in charge of making the final decision of PU channel state through one of the decision rules (only hard decision rules are considered, soft decision is out of the scope for this work) and then exploit the sequence of reported idle/busy channel states to estimate the durations of the channel holding times T_0/T_1 and the statistics (i.e., distribution). The considered system model is shown in in Fig. 1.

The cooperative estimation can be sub-characterised into four indispensable stages. Starting with the sensing stage, every SU performs spectrum sensing on a regular basis to estimate the primary channel availability. Second stage is the local hard decision, every SU utilises a detection algorithm to generate the binary channel state decisions (0 for idle/absence of PU and 1 for busy/presence of PU). The decisions of all SUs are assumed to be independent. The third stage is the reporting phase, where the local decisions of every SU are reported to the central FC through a dedicated reporting channel for the final global decision, where the FC (CR base station) is in charge of the final global decisions while the SUs function as cooperative sensing nodes. At every sensing event (performed with a sensing period of T_s time units), the FC makes the global decisions regarding the presence/busy (H_1) or absence/idle (H_0) of a PU. The decision rules considered in this work are the most popular ones (AND, OR, MAJORITY) [36].

1) AND-rule: The FC decides that a PU is present only if all cooperative SUs report with PU present (i.e., all SUs report with 1).
2) OR-rule: The FC decides that a PU is present when at least one cooperative SU reports with PU present (i.e., at least one SU reports with 1).
3) MAJORITY-rule: The FC decides that a PU is present when half or more of the cooperative SUs decide the presence of a PU (i.e., $K/2$ or more SUs report with 1).

Based on one of these three hard decision rules the FC makes a decision on the PU channel state and then exploits the sequence of reported idle/busy channel states to estimate the durations of the channel holding times $\widetilde{T}_i$ ($i = 0$ for idle periods, $i = 1$ for busy periods) of the original primary busy/idle periods T_i. Note that the estimated periods are integer multiples of the employed sensing period (i.e., $\widetilde{T}_i = mT_s$, $m \in \mathbb{N}^+$) and as a result the estimated periods will differ from the true original periods, which can in general be assumed to have a continuous domain (i.e., $T_i \in \mathbb{R}^+$).

In practice, SUs can work under both low and high SNR conditions. Under low SNR, SUs suffer from sensing errors (on local decisions, as every SU contributes in the final decision). ISS occurs in two types of errors: false alarm ($\widetilde{H} = H_1|H_0$) which is characterised by the probability of false alarm (P_{fa}), where the PU signal is not present but announced as present because of the high noise level present at SU's receiver, and missed detection ($\widetilde{H} = H_0|H_1$) which is characterised by the probability of missed detection (P_{md}), where the PU signal is present but with power lower than the receiver's threshold because of fading and shadowing.

Sensing errors have a significant impact on the performance of cognitive network systems (both PUs and SUs) and on the estimation of PU traffic statistical information as well. Inaccurate detection leads to inaccurate estimation for PU traffic activity statistics as the estimated durations can be longer or shorter than the original values. Another source of error is MUs who report with fake channel states to confuse the FC and lead it to announce wrong global decisions, thus missing the opportunity of transmission and leading to inaccurate PU traffic estimations.

The main objective of this research is to study the cooperative estimation of the primary statistics (distribution of period durations) under spectrum sensing errors and SSDF attacks, and propose methods that can provide an accurate estimation of the PU traffic statistics under such challenging conditions.

III. COOPERATIVE ESTIMATION OF THE DISTRIBUTION OF PRIMARY CHANNEL HOLDING TIMES

Two methods are considered in this work for the estimation of the distribution of primary idle/busy periods, the Direct Estimation Method (DEM) and the Method of Moments (MoM).

A. DIRECT ESTIMATION METHOD (DEM)

The direct estimation of the distribution is based on the empirical cumulative distribution function (ecdf in MATLAB), where the Kaplan-Meier estimation is obtained utilising the ecdf function for the given samples. The main advantage of this method is that it requires no prior knowledge about the primary distribution. The main drawback of this method is that the estimated distribution is a discrete version of the original continuous distribution as the estimated periods are discrete (integer) multiples of the sensing period T_s. Moreover, this method can not achieve high accuracy for all sensing periods, which can not be improved even by increasing the number of SUs as it will be seen in the results section. This motivates the consideration of the following method.

B. METHOD OF MOMENTS (MOM)

To overcome the limitations of the DEM, a solution based on the MoM is considered. For the MoM, the distribution of the primary periods has to be known or assumed to be known. The distribution parameters are then estimated from

the sample moments. The probability density function (PDF) and cumulative density function (CDF) for the exponential distribution are given by [37]:

$$f_{T_i}(t) = \begin{cases} 0 & t < \mu_i \\ \lambda_i e^{-\lambda_i (t-\mu_i)} & t \geq \mu_i \end{cases} \quad (1)$$

$$F_{T_i}(t) = \begin{cases} 0 & t < \mu_i \\ 1 - e^{-\lambda_i (t-\mu_i)} & t \geq \mu_i \end{cases} \quad (2)$$

where $\lambda_i \geq 0$ is the scale parameter of the distribution and $\mu_i > 0$ is the location parameter (also the smallest value for the PU activity period. i.e., $T_i \geq \mu_i$) .

The distribution parameters can be estimated following three approaches:

1) Direct estimation of minimum

The minimum period $\widetilde{\mu}_i^{dem}$ can be estimated as:

$$\widetilde{\mu}_i^{dem} = \min\left(\{\widetilde{T}_i\}_{n=1}^{N}\right) = T_s \quad (3)$$

where $\{\widetilde{T}_{i,n}\}_{n=1}^{N}$ is a set of N observed periods and its minimum value under ISS is given by T_s as discussed in [16]. The value of λ_i can be inferred from:

$$\widetilde{\mathbb{V}}(T_i) = \frac{1}{\lambda_i^2} \approx \frac{1}{N-1}\sum_{n=1}^{N}\left[\widetilde{T}_{i,n} - \mathbb{E}(\widetilde{T}_i)\right]^2 \quad (4)$$

where $\widetilde{\mathbb{V}}(T_i)$ is the variance of the observed PU periods and $\mathbb{E}(\widetilde{T}_i)$ is the mean which is given by (5).

2) Minimum based on MoM

In general, the higher the number of SUs for the cooperative estimation of mean and variance, the higher the accuracy of the estimation. This observation can be utilised to estimate μ_i as follows:

$$\mathbb{E}(\widetilde{T}_i) = \widetilde{\mu}_i + \frac{1}{\lambda_i} \approx \frac{1}{N}\sum_{n=1}^{N}\widetilde{T}_{i,n} \quad (5)$$

$$\widetilde{\mu}_i = \mathbb{E}(\widetilde{T}_i) - \sqrt{\widetilde{\mathbb{V}}(T_i)} \quad (6)$$

where $\mathbb{E}(\widetilde{T}_i)$ is the mean of the observed PU periods and $\mathbb{V}(\widetilde{T}_i)$ is their variance.

3) Minimum based on modified MoM

A similar procedure as above is utilised, but with a correction factor to reduce the effects of finite spectrum sensing period. The estimation of $\widetilde{\mathbb{V}}(T_i)$ is given by:

$$\widetilde{\mathbb{V}}(T_i) = \frac{1}{\lambda_i^2} - \frac{T_s^2}{6} \approx \frac{1}{N-1}\sum_{n=1}^{N}\left[\widetilde{T}_{i,n} - \mathbb{E}(\widetilde{T}_i)\right]^2 - \frac{T_s^2}{6} \quad (7)$$

where $T_s^2/6$ is the correction factor introduced in [38] to remove the effect of the finite sensing period T_s.

While the main difference among the methods described above is the ability to remove the impact of using a finite sensing period on the estimated distribution, another important aspect of practical importance is how the presence of sensing errors affects the accuracy of the estimated distribution for each method. An adequate study of this aspect from an analytical point of view would need to take into account not only the probabilities of errors but also other more complex aspects such as the (random) number of errors and their (random) relative locations within each PU period, since this determines how the original PU periods would be split into shorter periods as explained in [16], and how the errors are correlated. An adequate analytical treatment of this specific problem requires a separate study that is out of the scope of this work and is suggested as future work. The impact of sensing errors will be illustrated in this work in Section VII based on a simulation approach.

IV. LOCAL STATE REPORTING METHODS AND OVERHEAD

Cooperation can improve the estimation of both the instantaneous channel state and the primary traffic statistics, however the cooperative process introduces signalling overhead, which reduces the spectrum and energy efficiencies. Reporting in every sensing event is in general necessary in the case of cooperative spectrum sensing but is not essential in the case of cooperative PU traffic estimation considered in this work. A possible increase in spectrum and energy efficiency can be achieved by reducing the amount of channel reports required at each sensing stage. In this section, first the original reporting mechanism is described followed by the On/Off reporting method proposed in [39], then a new method (differential reporting) is proposed.

A. PERIODIC REPORTING MECHANISM

In the default periodic reporting mechanism, every SU transmits a report containing the local decision (at every sensing event) during the reporting stage to the central FC. Each report is sent through a dedicated report channel for every SU. The periodic reporting is summarised in Algorithm 1. The main drawback with periodic reporting is the high number of reports as every SU sends reports to the FC with local decisions via its own dedicated reporting channel in every single sensing event.

Algorithm 1: Periodic reporting

Input : $\lambda \in \mathbb{R}^+$ ▷ Energy decision threshold
$N_s \in \mathbb{N}^+$ ▷ Number of signal samples
Output: $R_{ch,i} \in \{0, 1\}$ ▷ Channel state report

for *each sensing event* i **do**
  $Y_i \leftarrow$ Energy of N_s samples ▷ Energy detection
  if $Y_i \geq \lambda$ **then**
    $R_{ch,i} \leftarrow 1$ ▷ Flag channel as busy
  else
    $R_{ch,i} \leftarrow 0$ ▷ Flag channel as idle
  end
  SU sends $R_{ch,i}$ to FC
end

Algorithm 2: On/Off reporting

Input : $\lambda \in \mathbb{R}^+$ ▷ Energy decision threshold
$N_s \in \mathbb{N}^+$ ▷ Number of signal samples
Output: $R_{ch,i} \in \{0, 1\}$ ▷ Channel state report

for *each sensing event* i **do**
  $Y_i \leftarrow$ Energy of N_s samples ▷ Energy detection
  if $Y_i \geq \lambda$ **then**
    $R_{ch,i} \leftarrow 1$ ▷ Flag channel as busy
    SU sends $R_{ch,i}$ to FC
  else
    $R_{ch,i} \leftarrow 0$ ▷ Flag channel as idle
    SU remains silent
  end
end

B. ON/OFF REPORTING MECHANISM

In this method, which is proposed in [39], all SUs report the local states back to the FC only during busy periods and remain silent during idle periods. This way the reporting overhead would be reduced from the periodic reporting, especially at low channel usage (i.e., low duty cycle). An alternative approach is to report the local states back to the FC only during idle periods and remain silent otherwise. This way the reporting overhead would be reduced from the periodic reporting under high channel usage (i.e., high duty cycle). The reporting option that provides the lowest number of reports depends on whether the duty cycle is lower than 0.5 (reporting during busy periods) or greater (reporting during idle periods). If the primary channel duty cycle is around 0.5, then both options are equivalent. In practice, SUs target primary channels with limited primary usage. As a result, only the first case for the On/Off reporting mechanism (i.e., reporting during busy periods) will be considered for comparison purposes in this work. The considered On/Off reporting is summarised in Algorithm 2.

Algorithm 3: Differential reporting

Input : $\lambda \in \mathbb{R}^+$ ▷ Energy decision threshold
$N_s \in \mathbb{N}^+$ ▷ Number of signal samples
Output: $R_{ch,i} \in \{0, 1\}$ ▷ Channel state report

for *each sensing event* i **do**
  $Y_i \leftarrow$ Energy of N_s samples ▷ Energy detection
  if $Y_i \geq \lambda$ **then**
    $R_{ch,i} \leftarrow 1$ ▷ Flag channel as busy
  else
    $R_{ch,i} \leftarrow 0$ ▷ Flag channel as idle
  end
  if $R_{ch,i} = R_{ch,i-1}$ *(i.e., same as previous state)* **then**
    SU remains silent
  else
    SU sends $R_{ch,i}$ to FC
  end
end

C. PROPOSED DIFFERENTIAL REPORTING MECHANISM

A differential reporting method is proposed where, in contrast to periodic reporting, SUs report their local decisions only when there is a change in the locally detected PU state (i.e., bit 1 is sent when the local decision goes from idle to busy and bit 0 is sent when the local decision goes from busy to idle). When SUs remain silent, the FC assumes that the new detected state is the same as the last reported state. The differential reporting mechanism is summarised in Algorithm 3. For differential reporting, the FC needs to keep a copy of every SU last state (for comparison with new sensed states) to estimate the PU period durations.

The differential reporting mechanism is expected to have a significant impact on the reporting overhead by reducing the amount of required reports and therefore increase the total system efficiency. This will be discussed in detail in Section VII.

D. ANALYSIS OF THE REQUIRED NUMBER OF REPORTS

Closed form expressions for the expected number of reports for the periodic, On/Off and differential reporting mechanisms are derived for two scenarios: first under perfect spectrum sensing ($P_{fa} = P_{md} = 0$), then under imperfect spectrum sensing (P_{fa}, $P_{md} > 0$).

First, the expected number of reports n_p for the periodic reporting mechanism, at both high SNRs (Perfect Spectrum Sensing, PSS) and low SNRs (Imperfect Spectrum Sensing, ISS) scenarios, is given by:

$$E\{n_p\} = \frac{E\{T_1\}}{T_s}\frac{N}{2} + \frac{E\{T_0\}}{T_s}\frac{N}{2} \tag{8}$$

where $N \in \mathbb{N}^+$ is the total number of idle and busy periods in the observed set $\{\widetilde{T}_{i,n}\}_{n=1}^{N}$, $E\{T_0\}$ and $E\{T_1\}$ are the expected durations of idle and busy periods, respectively,

and T_s is the sensing period. Notice that P_{fa} and P_{md} do not affect the total amount of reports since in the periodic reporting case a report is always sent in every sensing event.

Second, for the On/Off reporting mechanism (which only reports during busy periods), the expected number of reports n_{of} under PSS is given by:

$$E\{n_{of}\} = \frac{E\{T_1\}}{T_s}\frac{N}{2} \tag{9}$$

while it can be easily seen that for ISS the expected number of reports is given by:

$$E\{n_{of}\} = \frac{E\{T_1\}}{T_s}\frac{N}{2}(1-P_{md}) + \frac{E\{T_0\}}{T_s}\frac{N}{2}P_{fa} \tag{10}$$

Lastly, for the differential reporting mechanism, the expected number of reports n_d under PSS is given by:

$$E\{n_d\} = N \tag{11}$$

since under high SNR, the total number of reports sent to the FC is the same as the total number of periods, as one report is sent for every new observed period. On the other hand, an upper bound for the expected number of reports for differential reporting under ISS is found as follows:

$$E\{n_d\} = N + N\left[\frac{E\{T_1\}}{T_s}P_{md} + \frac{E\{T_0\}}{T_s}P_{fa}\right] \tag{12}$$

notice that one error (either false alarm or missed detection) will result in two reports. The upper bound in (12) is loose and can be approximated by taking into consideration the effect of the sensing error position within the period. For instance, consecutive sensing errors within the same period or sensing errors occurring at beginning or ending of the period result in a single report, then the following expression is obtained:

$$\begin{aligned} E\{n_d\} =& N + N\left[\frac{E\{T_1\}}{T_s}P_{md} + \frac{E\{T_0\}}{T_s}P_{fa}\right] - \\ &- NP_{md} - \sum_{k=2}^{\lfloor E\{T_1\}/T_s\rfloor}\frac{N}{2}\frac{E\{T_1\}}{T_s}P_{md}^k - \\ &- NP_{fa} - \sum_{k=2}^{\lfloor E\{T_0\}/T_s\rfloor}\frac{N}{2}\frac{E\{T_0\}}{T_s}P_{fa}^k \end{aligned} \tag{13}$$

The previous analytical results are for a single CR and can be easily scaled up by multiplying by the number of cooperative SUs K.

V. SPECTRUM SENSING DATA FALSIFICATION

In previous sections, all cooperative users are assumed to be honest. Unfortunately, given the openness nature of wireless communications, cognitive networks and advances in software defined radios have made the system vulnerable to data falsification attacks carried out by malicious or greedy nodes disguised [40]. MUs will send falsified reports. This type of attack is known as SSDF [25]. MUs have two main objectives for attacks [41]: first is to interfere with the primary system by having MUs report with idle states at busy primary channels, second is to report with busy states when local sensing decisions provide an idle state and, as a result, the FC falsely declares the primary channel as busy so that legitimate SUs have to wait for another sensing event. Meanwhile, MUs can access the idle channel exclusively. This attack strategy is typically utilised by greedy MUs to maximise their data rate. In this work, the main focus is on the later scenario.

A. SPECTRUM SENSING DATA FALSIFICATION ATTACKS

In this work, the considered SSDF attacks are similar to the ones described in [29], [42], [43]. Intelligent attacks such as those in [44] are out of scope of this work. The considered SSDF attacks are:

1) Blind attack: The attackers report with busy state in every sensing event [25].
2) Random attack: The MUs attack (i.e., report an idle channel as busy) with a given probability of attack $P_a < 1$ [45].

The blind attack would have a devastating effect on the resulting global detection if it succeeds, however its detection is straightforward. Notice that under periodic and On/Off reporting, the MU would report a busy PU channel in 100% of the submitted reports, while under differential reporting the MU would indicate the channel as busy in the initial report and then would not report anymore, implying that the channel still remains busy. These extreme cases would be very easy to detect by the FC by simply counting the number of reports and states sent by each user and comparing with the rest of users (taking into account the employed reporting mechanism). As a result, a modified version of the pure blind attack is here considered (see Algorithm 4), which is more sophisticated and therefore increases the chances of this type of attack to succeed. Notice that this modified blind attack requires MUs to sense the PU channel before sending a report to the FC, while the pure blind attack would not require any sensing at all. The random attack (Algorithm 5) also requires MUs to sense the PU channel before sending a report (regardless of the reporting mechanism employed) since the actual states of the PU channel need to be known in order to meet the desired probability of attack (P_a). Therefore, in both types of attack (blind and random) MUs need to sense the channel before sending the report to the FC.

For the case of differential reporting, in order to be able to apply SSDF attacks successfully, MUs need to follow the reporting rules imposed by the FC. Not following the reporting rules would lead to anomalous sequences of reports, with much higher/lower number of reports than the average, which would make the attack process susceptible of being detected by the FC. Thus, it is essential for MUs to follow the same reporting procedure imposed by the FC.

Finally, it is also worth mentioning that MUs may attack not only during the idle periods of the PU channel (by sending a busy report), but also during the busy periods of the

Algorithm 4: Modified blind attack (with differential reporting)

Input : $\lambda \in \mathbb{R}^+$ ▷ Energy decision threshold
$N_s \in \mathbb{N}^+$ ▷ Number of signal samples
Output: $R_{ch,i} \in \{0,1\}$ ▷ Channel state report

for *each sensing event* i **do**
  $Y_i \leftarrow$ Energy of N_s samples ▷ Energy detection
  if $Y_i \geq \lambda$ **then**
    $R_{ch,i} \leftarrow 1$ ▷ Flag channel as busy
  else
    $R_{ch,i} \leftarrow 0$ ▷ Flag channel as idle
  end
  if $R_{ch,i} = R_{ch,i-1}$ *(i.e., same as previous state)* **then**
    MU remains silent
  else
    MU sends $R_{ch,i} = 1$ to FC
  end
end

PU channel (by sending an idle report), or a combination of both. While attacks during PU busy periods may be possible, in this case the MU does not obtain an individual benefit from leading the FC to believe that the channel is idle when it is actually busy and therefore the MU does not have a strong incentive to carry out such attack. On the other hand, leading the FC to believe that the channel is busy when it is actually free allows the MU to prevent other SUs from transmitting and hence use the PU channel idle times for its own transmissions. Therefore the MU does have a strong incentive to attack during idle periods (by sending a busy report), which is not the case during busy periods. Notice that the algorithms and analyses presented in this work can be readily adapted to the either type of attack by simply reverting idle/busy periods (both in the algorithms and analysis of results). However, in order to simplify the subsequent analysis and discussion, we restrict ourselves, without loss of generality, to the case where MUs attack during idle periods only.

B. PROPOSED ALGORITHM

To eliminate the effects of SSDF attacks, a secure and efficient data fusion is essential, which in turn requires a reliable defence reference to identify MUs [42]. However in practical scenarios, a reliable reference is not always available. Eventually honest reports are mixed with malicious ones. In this context, we propose a novel algorithm to identify contrived MUs reports without the requirement of a previous reference. The key idea, which is shown in Algorithm 6, is based on the differential reporting mechanism. Whenever a report is available at the FC from a specific SU, a comparison is made with the previous report from the same SU. If the report contains information of same state as the previous report, then the report is discarded and the decision rule is applied based on the reports from the other $K-1$ SUs. Furthermore, the proposed algorithm can almost function in

Algorithm 5: Random attack (with differential reporting)

Input : $\lambda \in \mathbb{R}^+$ ▷ Energy decision threshold
$N_s \in \mathbb{N}^+$ ▷ Number of signal samples
Output: $R_{ch,i} \in \{0,1\}$ ▷ Channel state report

for *each sensing event* i **do**
  $Y_i \leftarrow$ Energy of N_s samples ▷ Energy detection
  if $Y_i \geq \lambda$ **then**
    $R_{ch,i} \leftarrow 1$ ▷ Flag channel as busy
  else
    $R_{ch,i} \leftarrow 0$ ▷ Flag channel as idle
  end
  if $R_{ch,i} = R_{ch,i-1}$ *(i.e., same as previous state)* **then**
    MU remains silent
  else
    MU generates a radom number $Z \sim U(0,1)$
    if $Z < P_a$ **then**
      MU sends $R_{ch,i} = 1$ to FC
    else
      MU sends $R_{ch,i}$ to FC
    end
  end
end

Algorithm 6: Defence against attackers (with differential reporting)

Input : Reports from sensing nodes
Output: Decision

for *each report* $R_{k,i}$ *from* SU_k *in sensing event* i **do**
  if $R_{k,i} = R_{k,i-1}$ **then**
    $R_{k,i}$ is discarded
    Apply MAJORITY rule to $K-1$ SUs
  else
    Apply MAJORITY rule to K SUs
  end
end

real-time without the need for a comparison with statistical characteristics for sensors as the operation of obtaining accurate statistical information requires a significant sample size [15]. The proposed algorithm differs from the literature in that it is much simpler and does not require any pre-defined trusted nodes nor sophisticated rules at the FC.

VI. SIMULATION AND EXPERIMENTAL METHODOLOGY

The performance of the considered methods was evaluated both with simulations and hardware experiments. Simulations were performed in MATLAB by generating several sequences with a sufficiently large number of interleaved on/busy and off/idle periods from an exponential distribution. The simulation procedure can be summarised as follows:

1) Generate idle/busy periods' lengths T_i following an exponential distribution with predefined location (μ_i) and scale (λ_i) parameters.

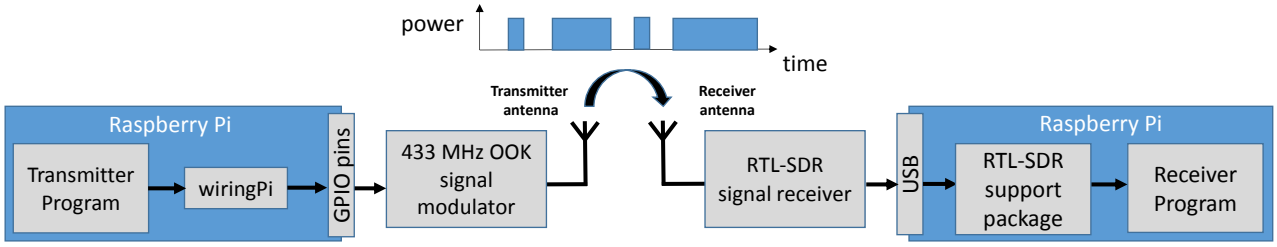


FIGURE 2: Block diagram of the PECAS prototype employed for hardware experiments [46].

2) Perform idle/busy sensing decisions H_0/H_1 on the generated sequence in step 1 every T_s time units (t.u.).
3) Calculate the idle/busy lengths estimated under PSS.
4) Add random errors (with $P_{fa} > 0$ and $P_{md} > 0$) in the sequence resulting from step 2.
5) Using the new H_0/H_1 sequence from step 4, calculate the period lengths $\widetilde{T}_i$ that would be estimated under ISS.
6) MUs will fake H_0 to H_1 with a given attack probability of $P_a > 0$.
7) FC computes the CDF of the idle/busy lengths obtained in steps 5 & 6 by applying a hard decision rule and compares with the CDF of the original periods.

The hardware experiments were conducted with a Prototype for the Estimation of Channel Activity Statistics (PECAS) [46]. This prototype is implemented with common low-cost components with the aim to reproduce a realistic scenario with inexpensive CR devices and introduce typical hardware sources of error and inaccuracies. This prototype is based on free open source code[1].

The hardware experiments are based on the same principle as the simulations but using a real transmitter and a real receiver. The block diagram is shown in Fig. 2. The transmitter (primary user) sends a sequence of exponentially-distributed idle/busy periods utilising a 433 MHz ON-OFF Keying (OOK) modulator with an output power of 2 dBm (controlled from a C program based on the *wiringPi* library). The receiver (secondary DSA/CR user), placed 1 metre apart, uses an RTL-SDR Software-Defined Radio (SDR) with a gain of 20 dB to monitor the transmitter activity (idle/busy) at 433 MHz every T_s seconds. At every sensing event, signal samples are captured at a sample rate of 10^6 samples per second, which are processed to decide the instantaneous channel state (idle/busy) using energy detection. The outcomes of the energy detection decisions are used to estimate the durations of the observed idle/busy periods and compute the primary activity statistics. While transmitter and receiver are controlled by C programs running on the same Raspberry Pi microcomputer, both programs run independently without synchronisation (as it would be the case of primary/secondary users in a real scenario). Real-time operation is achieved by a patched version of the Linux kernel and running the programs as processes with real-time priority.

[1] Available at: www.lopezbenitez.es/misc/PECAS.zip

The energy detection threshold can be selected through one of the following criteria:

- To meet a specific probability of false alarm (P_{fa}). This method requires knowledge of the SU noise power. In practice, this can be achieved by keeping the receiver function on an empty frequency channel for a sufficient time (several minutes in PECAS [46]) then setting the threshold to maintain the desired P_{fa} [47].
- To meet a specific probability of missed detection. This method requires knowledge of the received primary SNR in addition to the device noise power [48].
- To minimise the combined error from P_{fa} and P_{md}. This method also requires the knowledge of both the device noise power and primary signal SNR [49].

A more detailed description of these methods can be found in [50]. Since it is difficult to set accurately the energy detection threshold to result in a specific P_{fa} and P_{md} with the RTL-SDR [46], the errors are introduced through emulations to the on/off periods received by the RTL-SDR.

Even though the original PECAS is designed for a single CR scenario, the experiments are repeated for the required number of SUs to produce different streams for every SU and emulate a cooperative estimation scenario.

VII. SIMULATION AND EXPERIMENTAL RESULTS

In this section, the analysis and validation of the proposed methods are provided. The value considered for each parameter is shown in the title of each figure in terms of generic time units (t.u.). In the case of experimental results, where a particular time unit needs to be selected according to the real-time capabilities of the employed hardware platform, the reference unit is the second (i.e., 1 t.u. = 1 second). First, different decision rules will be assessed, followed by different methods to assess the estimated primary distribution accuracy. The comparison between the estimated and original distributions is performed using the classic Kolmogorov-Smirnov (KS) distance [51], defined as:

$$D_{KS} = \sup_{T_i} \left| F_{T_i}(T_i) - F_{\widetilde{T}_i}(T_i) \right| \tag{14}$$

where $F_{T_i}(T_i)$ and $F_{\widetilde{T}_i}(T_i)$ represent the CDFs of the original and estimated periods, respectively.

Fig. 3 compares the estimation accuracy of the considered hard decision rules (AND, OR, MAJORITY) when the cooperative SUs use periodic reporting and the FC uses the DEM to estimate the CDF of busy periods. For comparison

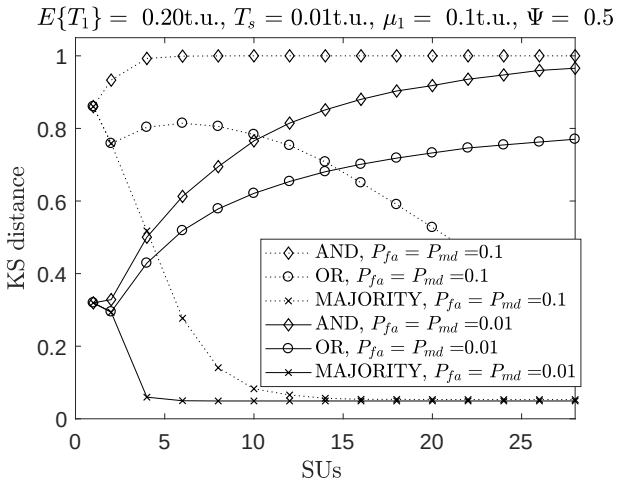


FIGURE 3: Accuracy of the estimated distribution for different fusion rules and periodic reporting under sensing errors.

purposes, the case of single SU is also included in Fig. 3. The duty cycle is set to 0.5 ($\Psi = 0.5$), where both busy and idle periods will have similar parameters. The MAJORITY rule outperforms the other rules in the estimation of the primary statistics (4 cooperative SUs can estimate accurately the primary statistics under $P_{fa} = P_{md} = 0.01$, while 12 SUs are required to estimate the primary statistics under $P_{fa} = P_{md} = 0.1$). As for the AND and the OR rules, both of them fail to provide an accurate estimation of the primary distribution (low KS distance value) for both scenarios of high and low sensing error probabilities. For the OR rule, the obtained results can be explained as any CR reports with a busy period will result in the FC announcing the channel as busy and as the number of cooperative SUs increases the probability of having false alarms increases as well. It is interesting to notice that the direct estimation of the CDF (i.e., DEM, which is considered in all cases in Fig. 3) never reaches a perfect accuracy ($D_{KS} = 0$) regardless of the number of SUs and the fusion rule. This is a result of the finite sensing period T_s [38]. Based on these results, further numerical results will only consider the MAJORITY fusion rule.

Fig. 4 shows the accuracy of the considered methods to estimate the distribution of the primary traffic for different sensing periods. Experimental results are considered only here due to the significant amount of time required to run experiments for cooperative SU scenarios using a single SU hardware platform. As it can be observed, the experimental results (with PECAS) provide a perfect fit with simulations. For small sensing periods (Fig. 4(a)), the DEM performs better than the MoM and its modified version in Section III-B3 (MMoM), but for high number of SUs, MoM and MMoM can provide a more accurate estimation. For higher sensing durations (Fig. 4(b) and Fig. 4(c)) MoM and MMoM provide better accuracy in the estimation of the primary traffic over the whole range of the number of cooperative SUs. The minimum period obtained from MMoM gives better estimation than the minimum obtained through the original MoM, except for the case where T_s has a small duration (i.e., multiple sensing events occur in a single period) where both minimums provide a similar KS distance. The direct estimated minimum with MoM provides results with significant inaccuracy regardless of the sensing period or the number of cooperative SUs. Since the MMoM performs better than the rest of methods, it will be the only method considered in the remainder of this section.

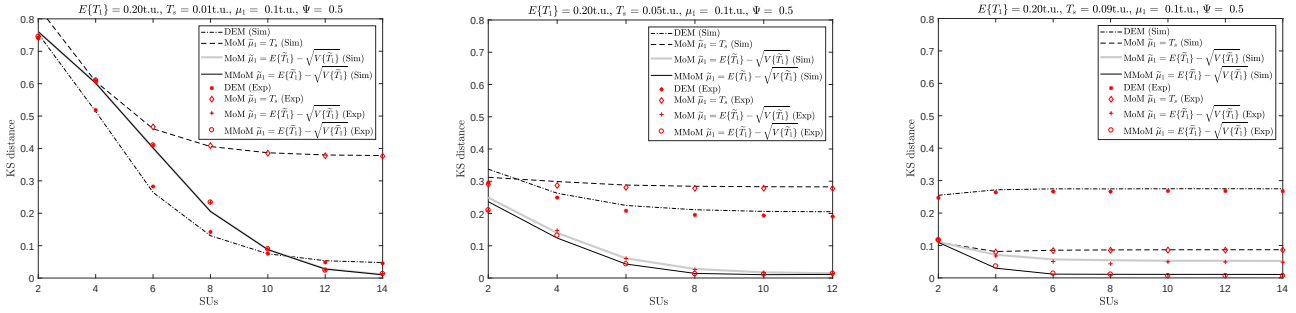
The performance of the periodic reporting, On/Off reporting and the proposed differential reporting mechanisms for cooperative estimation will be discussed based on the MAJORITY fusion rule with MMoM distribution estimation. As it can be appreciated in Fig. 5, the three considered methods have a similar performance under sensing errors, however the differential reporting mechanism provides higher efficiency and security advantages in comparison with the other methods as discussed below.

Fig. 6 shows the required number of channel reports for 20,000 periods for the three considered reporting mechanisms (periodic, On/Off and differential) under different primary loads (high Ψ = 0.75, moderate Ψ = 0.5 and low Ψ = 0.25). As it can be appreciated, the derived analytical expressions provide a perfect match for the periodic and On/Off reporting methods, while the result of (13) provides a tight upper bound for the required number of reports in the case of the differential reporting mechanism. The reduction in the amount of reports transmitted using the On/Off and differential reporting mechanisms with respect to the periodic reporting mechanism can be quantified, respectively, as:

$$B_{of} = \frac{E\{n_{of}\}}{E\{n_p\}} \tag{15}$$

$$B_d = \frac{E\{n_d\}}{E\{n_p\}} \tag{16}$$

where B_{of} and B_d are the reduction in the amount of reports for On/Off and differential reporting mechanisms respectively. The smaller the value of B_{of}/B_d , the lower the amount of reporting overhead required for feedback and therefore the higher the efficiency. Figs. 7 and 8 show the reduction in the amount of reports for On/Off and differential reporting mechanisms with respect to the periodic reporting mechanism under perfect and imperfect spectrum sensing scenarios, respectively. The scenario of perfect spectrum sensing is considered to give an idea on the reduction in the case of high primary signal power present at the SU. As it can be concluded from both figures, the differential reporting mechanism outperforms the On/Off in nearly every channel load, except for small duty cycles (Ψ = 0.25) and large sensing periods ($T_s > \frac{\mu_i}{2}$) as at low duty cycles the SUs will remain idle for most of the time due to the absence of PU traffic. As it can be observed, the best estimation accuracy obtained for smaller sensing periods. In practice, the duty cycle of PU is unknown and the differential reporting mechanism provides higher efficiency. As it can be appreciated,



(a) (b) (c)

FIGURE 4: Different methods to estimate the distribution under periodic reporting: (a) $T_s = 0.01$ t.u., (b) $T_s = 0.05$ t.u., (c) $T_s = 0.09$ t.u.

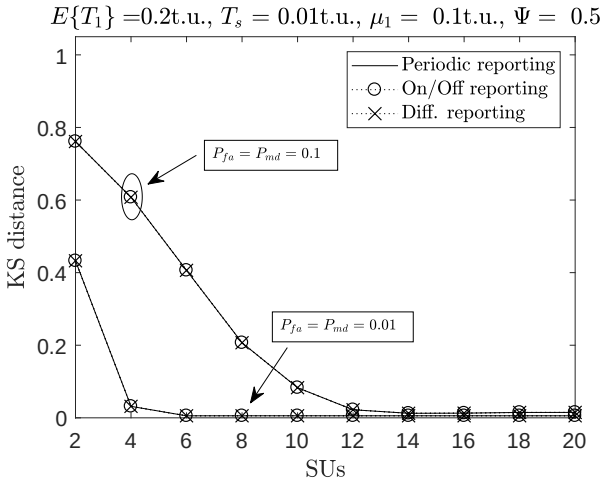


FIGURE 5: Accuracy of the estimated distribution for different reporting mechanisms.

the proposed mechanism reduces significantly the amount of required reports for all scenarios.

The accuracy of the estimation of primary traffic statistics under random attacks with different fusion rules is shown in Fig. 9. As it can be appreciated, the MAJORITY rule outperforms the AND/OR rules in the presence of attacks. The OR rule is ineffective against attacks because only one busy report is required to declare the channel as busy, therefore a single MU would be able to prevent the whole SU network from transmitting. The AND rule would be effective in an ideal case of perfect spectrum sensing, since a single honest SU who reports an idle channel as idle would be enough to make any attack fail, regardless of the number of MUs; however, in a realistic ISS scenario, the presence of sensing errors means that an idle channel may be reported as busy (false alarm) and vice versa (missed detection) even by honest SUs. Overall, the MAJORITY rule provides the best balance between malicious and erroneous reports, and therefore leads to the best estimation accuracy as observed in Fig. 9. By increasing the number of SUs, the MAJORITY rule enables an accurate estimation even under SSDF attacks. Comparing Figs. 3 and 9, it can be observed that the presence of MUs (Fig. 9) increases the total number of required SUs in order to achieve an accurate estimation of the distribution with the MAJORITY rule with respect to the case of no MUs (Fig. 3), however the MAJORITY rule still provides the best estimation accuracy. Similar conclusions are obtained in the case of blind attacks (not shown here for brevity). Therefore, the MAJORITY rule provides the best estimation accuracy, even in the presence of SSDF attacks. The subsequent performance analysis under SSDF attacks will consider the MAJORITY fusion rule only.

The accuracy of the estimation of primary traffic statistics under blind and random attacks is shown in Figs. 10 and 11 respectively. As it can be appreciated, the blind attack has the same level of degradation on the estimation of the PU distribution for the three reporting mechanisms (periodic, On/Off and differential). Moreover, when the population of attackers becomes half of the SUs (Fig. 10(a)), the FC will be overwhelmed with wrong reports and produce false global decisions regardless of the probability of missed detection and false alarm. For smaller MUs population (Fig. 10(c)), a large number of SUs is required to produce an accurate estimation of the primary statistics. The random attack has less severe effects on the estimation of the statistics in comparison with the blind attack. In fact, the blind attack is a special case of the random attack with attack probability $P_a = 1$. In general, the differential reporting mechanism performs better than the periodic and On/Off counterparts regardless of the P_a value. Nevertheless, all methods fail to provide an accurate estimation of the PU statistics except for small P_a (Fig. 11(a)), where a high number of SUs are essential to have a relatively acceptable estimation (SUs $>$ 20). As it can be appreciated from Fig. 12, the proposed defense algorithm can significantly improve the estimation of primary statistics while mitigating the effects of MUs by discarding the contrived reports and keeping the correct ones for the cooperative estimation. Moreover, the proposed method provides accurate results regardless of the attack type or the population of MUs.

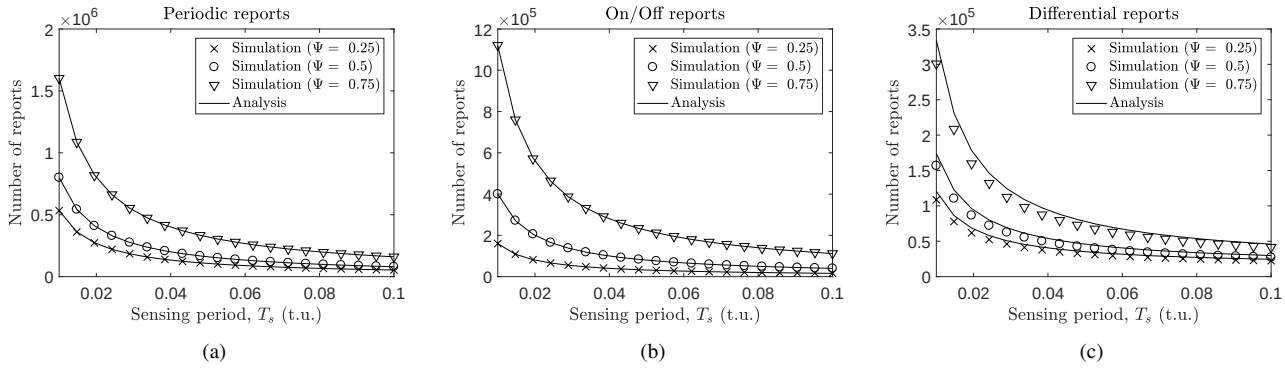


FIGURE 6: Required number of reports under sensing errors ($P_{fa} = P_{md} = 0.1$) for: (a) Periodic reporting, (b) On/Off reporting, (c) Differential reporting.

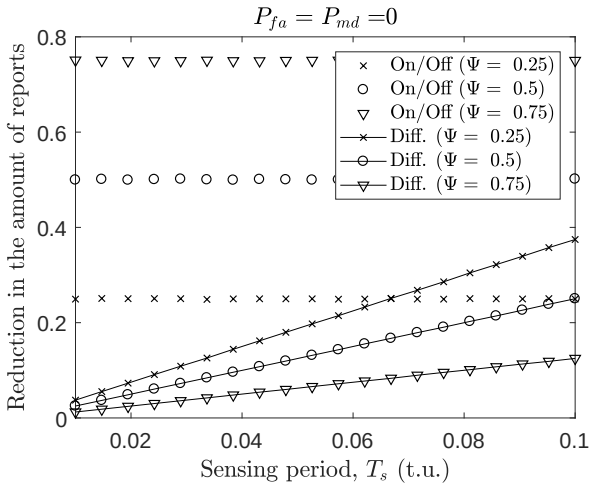


FIGURE 7: Reduction in the number of reports under PSS ($P_{fa} = P_{md} = 0$).

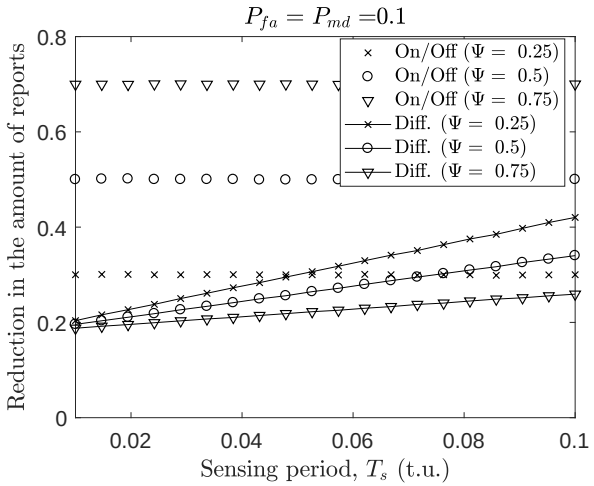


FIGURE 8: Reduction in the number of reports under ISS ($P_{fa} = P_{md} = 0.1$).

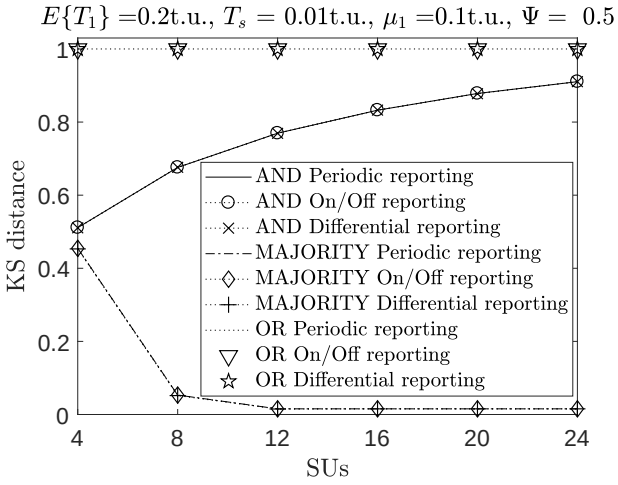


FIGURE 9: Accuracy of the estimated distribution for different fusion rules under both ISS ($P_{fa} = P_{md} = 0.01$) and random attacks (MUs = $K/4$, $P_a = 0.75$).

VIII. CONCLUSIONS

CR systems can benefit from the knowledge of PU activity statistics, which can be exploited to prevent interference and access the spectrum more efficiently. This information can be obtained individually by each CR user based on its local spectrum sensing observations, however a cooperative estimation approach can provide significant benefits both in terms of accuracy (overcoming the degrading effects of sensing errors) and reliability (overcoming the degrading effects of malicious users). In this context, this work has provided a detailed study on the cooperative estimation of the PU activity statistics (in particular, the distribution of the channel holding times) under both spectrum sensing errors and SSDF attacks. This study has evaluated the impact on the accuracy of the estimated statistics that several aspects may have, such as the hard decision rule used for cooperative sensing-based estimation (the MAJORITY rule was observed to provide the best performance) and the method employed to estimate the distribution (the MMoM approach proposed in this work has been proven to provide the most accurate estimation). While cooperative estimation can improve the estimation accuracy, it also increases the amount of signalling in the system (associated with the reporting overhead) and introduces security threads (from MUs deliberately sending incorrect reports). Both issues have been successfully addressed in this work by proposing a differential reporting mechanism that can decrease significantly the signalling overhead as well as a de-

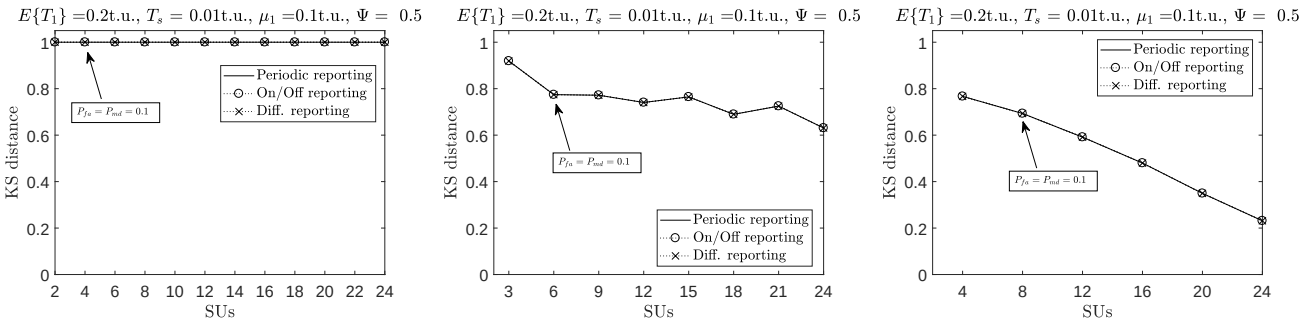


FIGURE 10: Accuracy of the estimated distribution under blind attacks: (a) MUs = $K/2$, (b) MUs = $K/3$, (c) MUs = $K/4$.

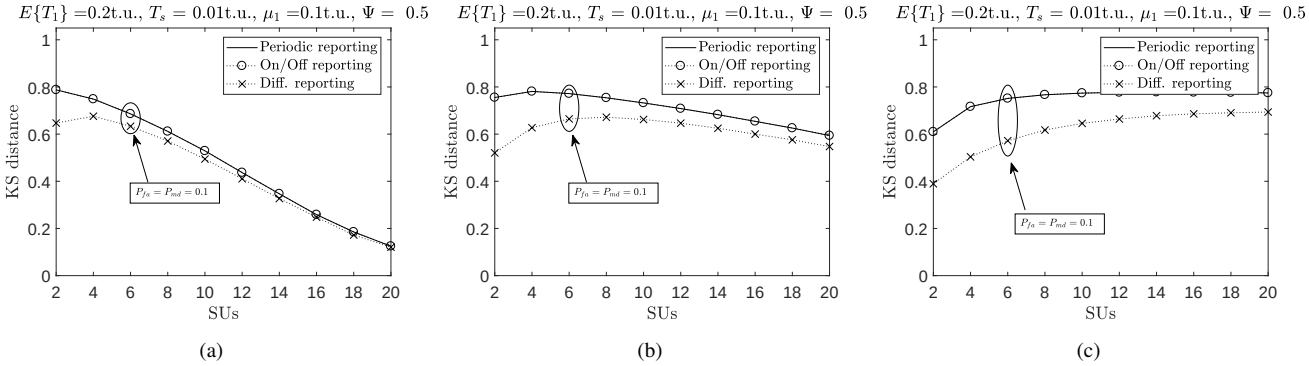


FIGURE 11: Accuracy of the estimated distribution under random attacks: (a) MUs = $K/2$ and $P_a = 0.25$, (b) MUs = $K/2$ and $P_a = 0.5$, (c) MUs = $K/2$ and $P_a = 0.75$.

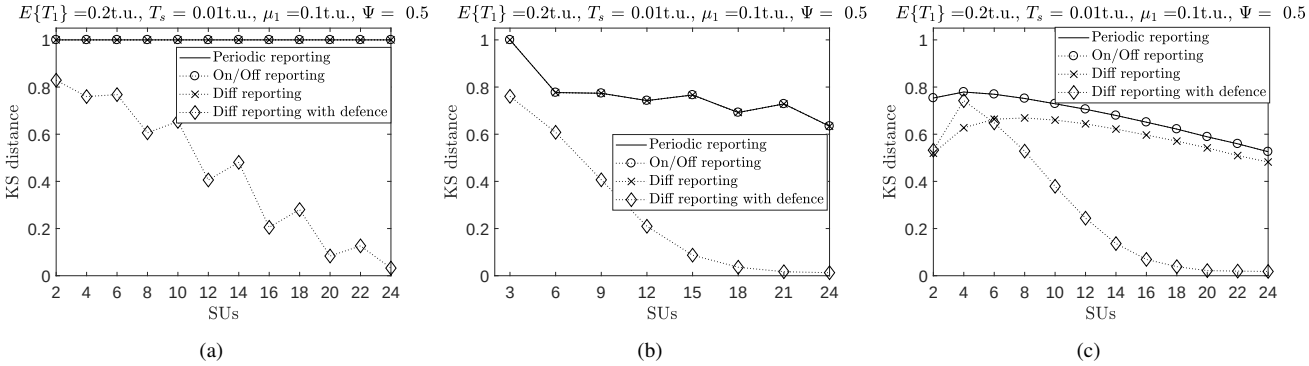


FIGURE 12: Accuracy of the estimated distribution under SSDF attacks with the proposed defence method: (a) MUs = $K/2$ and $P_a = 1$ (blind attack), (b) MUs = $K/3$ and $P_a = 1$ (blind attack), (c) MUs = $K/2$ and $P_a = 0.5$ (random attack).

fence mechanism that can effectively remove both blind and random SSDF attacks. The obtained simulation and experimental results demonstrate that the methods proposed in this work enable a more accurate estimation of the PU activity statistics with a reduced level of signalling overhead and a high level of security against SSDF attacks. Future extension to the presented work is to pair the differential reporting mechanism with other defence algorithms to tackle more sophisticated and intelligent attacks performed by MUs.

ACKNOWLEDGEMENTS

M. López-Benítez would like to thank the financial support received from British Council under UKIERI DST Thematic Partnerships 2016-17 (ref. DST-198/2017). K. Umebayashi would like to thank the supports received from the JSPS KAKENHI Grant Numbers 18K04124.

REFERENCES

[1] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," IEEE Personal Communications, vol. 6, no. 4, pp. 13–18, Aug 1999.

[2] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," IEEE J. Sel. Areas Comms., vol. 23, no. 2, pp. 201–220, Feb. 2005.

[3] M. López-Benítez and F. Casadevall, Spectrum Usage Models for the Analysis, Design and Simulation of Cognitive Radio Networks. Dordrecht: Springer Netherlands, 2012, pp. 27–73.

[4] M. Wellens, J. Riihijärvi, and P. Mähönen, "Empirical time and frequency domain models of spectrum use," Physical Communication, vol. 2, no. 1, pp. 10 – 32, 2009.

[5] X. Liu, B. Krishnamachari, and H. Liu, "Channel selection in multi-channel opportunistic spectrum access networks with perfect sensing," in Proc. 2010 IEEE Int'l. Symp. Dyn. Spect. Access Networks (DySPAN 2010), Apr. 2010, pp. 1–8.

[6] V. Southivong and T. Fujii, "Primary and secondary identification using energy detection with statistical primary information," in 2015 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), March 2015, pp. 164–169.

[7] C. H. Liu, W. Gabran, and D. Cabric, "Prediction of exponentially distributed primary user traffic for dynamic spectrum access," in 2012 IEEE Global Communications Conference, Dec 2012, pp. 1441–1446.

[8] K. Umebayashi, K. Hayashi, and J. J. Lehtomäki, "Threshold-setting for spectrum sensing based on statistical information," IEEE Communications Letters, vol. 21, no. 7, pp. 1585–1588, July 2017.

[9] M. Ghaznavi and A. Jamshidi, "Defence against primary user emulation attack using statistical properties of the cognitive radio received power," IET Communications, vol. 11, no. 9, pp. 1535–1542, 2017.

[10] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," IEEE Communications Surveys Tutorials, vol. 11, no. 1, pp. 116–130, First 2009.

[11] Q. Zhao, S. Geirhofer, L. Tong, and B. M. Sadler, "Opportunistic spectrum access via periodic channel sensing," IEEE Transactions on Signal Processing, vol. 56, no. 2, pp. 785–796, Feb 2008.

[12] K. Umebayashi, K. Moriwaki, R. Mizuchi, H. Iwata, S. Tiiro, J. J. Lehtomäki, M. López-Benítez, and Y. Suzuki, "Simple primary user signal area estimation for spectrum measurement," IEICE Transactions on Communications, vol. 99, no. 2, pp. 523–532, 2016.

[13] J. Lehtomäki, M. López-Benítez, K. Umebayashi, and M. Juntti, "Improved channel occupancy rate estimation," IEEE Transactions on Communications, vol. 63, no. 3, pp. 643–654, March 2015.

[14] A. Al-Tahmeesschi, M. López-Benítez, K. Umebayashi, and J. Lehtomäki, "Analytical study on the estimation of primary activity distribution based on spectrum sensing," in Proc. 28th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2017), Workshop on Cognitive Radio and Innovative Spectrum Sharing Paradigms for Future Networks (CRAFT 2017), Montreal, Quebec, Canada, 8-13 Oct. 2017, pp. 1–5.

[15] M. López-Benítez and J. Lehtomäki, "On the sensing sample size for the estimation of primary channel occupancy rate in cognitive radio," in Proc. IEEE Wireless Comms. and Networking Conf. (WCNC 2016), Apr. 2016, pp. 2599–2604.

[16] M. López-Benítez, "Can primary activity statistics in cognitive radio be estimated under imperfect spectrum sensing?" in 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Sept 2013, pp. 750–755.

[17] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," Physical Communication, vol. 4, no. 1, pp. 40 – 62, 2011.

[18] G. Amir and E. S. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," vol. 2, no. 2, pp. 71–82, Mar 2007.

[19] K. CichoÅĎ, A. Kliks, and H. Bogucka, "Energy-efficient cooperative spectrum sensing: A survey," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 1861–1886, thirdquarter 2016.

[20] J. Imtiaz and D. Kim, "Energy-efficient management of cognitive radio terminals with quality-based activation," IEEE Communications Letters, vol. 21, no. 5, pp. 1171–1174, May 2017.

[21] J. R. Long, W. Wu, Y. Dong, Y. Zhao, M. A. T. Sanduleanu, J. F. M. Gerrits, and G. van Veenendaal, "Energy-efficient wireless front-end concepts for ultra lower power radio," in 2008 IEEE Custom Integrated Circuits Conference, Sept 2008, pp. 587–590.

[22] Z. Khan, J. Lehtomaki, K. Umebayashi, and J. Vartiainen, "On the selection of the best detection performance sensors for cognitive radio networks," IEEE Signal Processing Letters, vol. 17, no. 4, pp. 359–362, April 2010.

[23] K. Umebayashi, J. J. Lehtomäki, T. Yazawa, and Y. Suzuki, "Efficient decision fusion for cooperative spectrum sensing based on OR-rule," IEEE Transactions on Wireless Communications, vol. 11, no. 7, pp. 2585–2595, July 2012.

[24] H. Rowaihy, S. Eswaran, M. Johnson, D. Verma, A. Bar-noy, and T. Brown, "A survey of sensor selection schemes in wireless sensor networks," in In SPIE Defense and Security Symposium Conference on Unattended Ground, Sea, and Air Sensor Technologies and Applications IX, 2007.

[25] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," IEEE Communications Surveys Tutorials, vol. 17, no. 3, pp. 1342–1363, thirdquarter 2015.

[26] T. Zhao and Y. Zhao, "A new cooperative detection technique with malicious user suppression," in 2009 IEEE International Conference on Communications, June 2009, pp. 1–5.

[27] Y. Al-Mathehaji, S. Boussakta, M. Johnston, and H. Fakhrey, "Defeating SSDF attacks with trusted nodes assistance in cognitive radio networks," IEEE Sensors Letters, vol. 1, no. 4, pp. 1–4, Aug 2017.

[28] J. Wu, X. Li, T. Song, L. Zhang, M. Liu, and J. Hu, "Two-stage credit threshold on cooperative spectrum sensing to exclude malicious users in mobile cognitive radio networks," in 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), June 2017, pp. 1–6.

[29] N. Marchang, A. Taggu, and A. K. Patra, "Detecting byzantine attack in cognitive radio networks by exploiting frequency and ordering properties," IEEE Transactions on Cognitive Communications and Networking, pp. 1–1, 2018.

[30] H. Kim and K. G. Shin, "Efficient discovery of spectrum opportunities with MAC-layer sensing in cognitive radio networks," IEEE Transactions on Mobile Computing, vol. 7, no. 5, pp. 533–545, May 2008.

[31] W. Gabran, C.-H. Liu, P. Pawelczak, and D. Cabric, "Primary user traffic estimation for dynamic spectrum access," IEEE J. Sel. Areas Comms., vol. 31, no. 3, pp. 544–548, Mar. 2013.

[32] Q. Liang, M. Liu, and D. Yuan, "Channel estimation for opportunistic spectrum access: uniform and random sensing," IEEE Trans. Mobile Computing, vol. 11, no. 8, pp. 1304–1316, Aug. 2012.

[33] P. Tehrani, L. Tong, and Q. Zhao, "Asymptotically efficient multichannel estimation for opportunistic spectrum access," IEEE Trans. Signal Processing, vol. 60, no. 10, pp. 5347–5360, Oct. 2012.

[34] W. Saad, Z. Han, H. V. Poor, T. Basar, and J. B. Song, "A cooperative bayesian nonparametric framework for primary user activity monitoring in cognitive radio networks," IEEE J. Sel. Areas Comms., vol. 30, no. 9, pp. 1815–1822, Oct. 2012.

[35] M. López-Benítez and F. Casadevall, "Time-dimension models of spectrum usage for the analysis, design, and simulation of cognitive radio networks," IEEE Transactions on Vehicular Technology, vol. 62, no. 5, pp. 2091–2104, Jun 2013.

[36] S. Kyperountas, N. Correal, and Q. Shi, "A comparison of fusion rules for cooperative spectrum sensing in fading channels," In Proceedings of the Wireless Symposium and Summer School, Blacksburg, VA, USA, 2âĂŞ4 June 2010.

[37] N. Johnson, S. Kotz, and N. Balakrishnan, Continuous univariate distributions, ser. Wiley series in probability and mathematical statistics: Applied probability and statistics. Wiley & Sons, 1995, no. v. 2.

[38] A. Al-Tahmeesschi, M. López-Benítez, J. Lehtomäki, and K. Umebayashi, "Accurate estimation of primary user traffic based on periodic spectrum sensing," in Proc. IEEE Wireless Comms. and Networking Conf. (WCNC 2018), Apr. 2018, pp. 1–6.

[39] S. Bae and H. Kim, "Robust cooperative sensing with on/off signaling over imperfect reporting channels," IEEE Transactions on Industrial Informatics, vol. 12, no. 6, pp. 2196–2205, Dec 2016.

[40] V. Selis and A. Marshall, "A classification-based algorithm to detect forged embedded machines in IoT environments," IEEE Systems Journal, pp. 1–11, 2018.

[41] O. Fatemieh, R. Chandra, and C. A. Gunter, "Secure collaborative sensing for crowd sourcing spectrum data in white space networks," in 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN), April 2010, pp. 1–12.

[42] L. Zhang, G. Ding, Q. Wu, and F. Song, "Defending against byzantine attack in cooperative spectrum sensing: Defense reference and performance analysis," IEEE Access, vol. 4, pp. 4011–4024, 2016.

[43] L. Zhang, Q. Wu, G. Ding, S. Feng, and J. Wang, "Performance analysis of probabilistic soft SSDF attack in cooperative spectrum sensing," EURASIP Journal on Advances in Signal Processing, vol. 2014, no. 1, p. 81, May 2014. [Online]. Available: https://doi.org/10.1186/1687-6180-2014-81

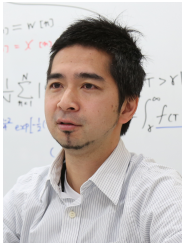
[44] W. Wang, L. Chen, K. G. Shin, and L. Duan, "Thwarting intelligent malicious behaviors in cooperative spectrum sensing," IEEE Transactions on Mobile Computing, vol. 14, no. 11, pp. 2392–2405, Nov 2015.
[45] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," IEEE Transactions on Signal Processing, vol. 59, no. 2, pp. 774–786, Feb 2011.
[46] M. López-Benítez, A. Al-Tahmeesschi, K. Umebayashi, and J. Lehtomaki, "PECAS: A low-cost prototype for the estimation of channel activity statistics in cognitive radio," in 2017 IEEE Wireless Communications and Networking Conference (WCNC), March 2017, pp. 1–6.
[47] S. Atapattu, C. Tellambura, and H. Jiang, "Spectrum sensing via energy detector in low SNR," in 2011 IEEE International Conference on Communications (ICC), June 2011, pp. 1–5.
[48] Y.-C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," IEEE Trans. Wireless Comms., vol. 7, no. 4, pp. 1326–1337, Apr. 2008.
[49] W. Zhang, R. K. Mallik, and K. B. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," IEEE Transactions on Wireless Communications, vol. 8, no. 12, pp. 5761–5766, December 2009.
[50] M. López-Benítez and J. Lehtomäki, "Energy detection based estimation of primary channel occupancy rate in cognitive radio," in 2016 IEEE Wireless Communications and Networking Conference, April 2016, pp. 1–6.
[51] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, Numerical recipes: The art of scientific computing, 3rd ed. Cambridge University Press, 2007.

AHMED AL-TAHMEESSCHI (S'16) received the B.Sc. and M.Sc. degrees in communications engineering from the University of Technology, Baghdad, Iraq, in 2009 and 2011, respectively. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, U.K. His research interests include cognitive radio networks, dynamic spectrum access techniques, algorithm design and machine learning.

MIGUEL LÓPEZ-BENÍTEZ (S'08, M'12, SM'17) received the B.Sc. and M.Sc. degrees in Telecommunication Engineering (both with Distinction) from Miguel Hernández University, Elche, Spain in 2003 and 2006, respectively, and a Ph.D. degree in Telecommunication Engineering (2011 Outstanding Ph.D. Thesis Award) from the Technical University of Catalonia, Barcelona, Spain in 2011. From 2011 to 2013, he was a Research Fellow in the Centre for Communication Systems Research of the University of Surrey, Guildford, UK. Since 2013, he has been a Lecturer (Assistant Professor) in the Department of Electrical Engineering and Electronics of the University of Liverpool, UK. His research interests include the field of wireless communications and networking, with special emphasis on cellular mobile communications and dynamic spectrum access in cognitive radio systems. He is/has been the principal investigator or co-investigator of research projects funded by the EPSRC, British Council and Royal Society, and has been involved in the European-funded projects AROMA, NEWCOM++, FARAMIR, QoSMOS and CoRaSat. He is Associate Editor of IEEE Access, IET Communications, and Wireless Communications and Mobile Computing, and has been a member of the Organising Committee for the IEEE WCNC International Workshop on Smart Spectrum (IWSS 2015-18). Please visit http://www.lopezbenitez.es for more details.

VALERIO SELIS (M'13) received the M.Sc. degree in computer science from Università degli Studi di Cagliari, Cagliari, Sardinia, Italy. He received his Ph.D. degree in electrical engineering and electronics from the University of Liverpool, Liverpool, U.K., in 2018. He is currently working as Research Associate with the Advanced Networks Research Group, University of Liverpool. Previous research experience saw him working, as a Research Assistant, on the "Cross-Layer Techniques for Intrusion Tolerant Network Design" project at Queen's University Belfast, Belfast, U.K. Moreover, since 2016, he has been a Development Director at Traffic Observation & Management (TOM) Ltd. TOM is a company specialised in intrusion detection & prevention systems for wireless networks. His research interests include wireless networks, Internet of Things, network security, trust management, and machine-to-machine communications.

DHAVAL K PATEL is currently working as Assistant Professor at School of Engineering and Applied Science - Ahmedabad University, India since 2014. He was also a visiting faculty at Franklin W. Olin College of Engineering-Massachusetts, USA. He worked as Junior Research Fellow in the Post Graduate Lab for Communication Systems at the Nirma University-India from 2011 to 2014. He received the B.E. and M.E. degrees in Communication Systems Engineering (both with Distinction/First-Class) from Gujarat University in 2003 and 2010, respectively, and a Ph.D. degree in Electronics and Communications from the Institute of Technology-Nirma University, India in 2014. His research area of interest includes Vehicular Cyber Physical System, 5G Wireless Networks, Non-parametric statistics and Physical Layer Security. He is the principal investigator of research projects funded by Department of Science and Technology (DST), UK-India Education and Research Initiative (UKIERI), Association of Southeast Asian Nations (ASEAN)-India Collaborative R&D Project and Gujarat Council on Science and Technology (GUJCOST).



KENTA UMEBAYASHI (S'00, M'04) received the LL.B. degree from Ritsumeikan University in 1996 and the B.E., M.E., and Ph.D. degrees from the Yokohama National University, Japan in 1999, 2001, and 2004, respectively. From 2004 to 2006, he was a research scientist at the University of Oulu, Centre for Wireless Communications (CWC). He is currently an associate professor at the Tokyo University of Agriculture and Technology. He was an associate editor of IEICE Transaction on Communications from May 2015 to May 2017. He was a principal investigator in the four Grants-in-Aid for Scientific Research projects and three Strategic Information and Communications R&D Promotion Programme projects. His research interests lie in the areas of signal detection and estimation theories for wireless communication, signal processing for multiple antenna systems, cognitive radio networks, and terahertz band wireless communication. He received the Best Paper Award at IEEE WCNC 2012 for a paper he authored, and the Best Paper Award at IEEE WCNC workshop IWSS 2015 for a paper he co-authored.